AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter.

1. (Currently Amended) A method of delivering a digital document to an intended recipient at a printout station, the method comprising:

receiving and securely retaining a transmitted document at the printout station;

receiving an independently verifiable data record of the intended recipient at the printout station;

obtaining a first token of the intended recipient;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient; and

releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token, wherein the retaining step comprises printing out the document as received and placing it in a locked compartment and the releasing step comprises a controller unlocking the compartment where the printed copy of the document is stored.

2. (Original) A method according to Claim 1, wherein the transmitted document is a fax document and the printout station comprises a fax machine.

3-6. (Canceled)

7. (Original) A method according to Claim 1, wherein the requesting step comprises requesting supply of data encoded with the second token which can be decoded with the first token.

8. (Original) A method according to Claim 1, wherein the releasing step is carried out when the intended recipient has presented a portable data carrier holding the second token to the printout station and has transferred data to prove their identity.

9. (Original) A method according to Claim 8, wherein the releasing step further comprises the intended recipient entering a verifiable security identifier into the printout station to establish that they are the legitimate owner of the portable data carrier.

10. (Original) A method according to Claim 8, wherein the portable data carrier is a smart card and the printout station comprises a smart card reader.

11. (Previously Presented) A method according to Claim 1, wherein the obtaining step comprises extracting the first token transmitted with the data record.

12. (Original) A method according to Claim 11, wherein the intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate.

13. (Original) A method according to Claim 1, further comprising carrying out an on-line check of the validity of the intended recipient's independently verifiable data record.

14. (Original) A method according to Claim 1, further comprising instructing a third party to carry out an on-line check of the validity of the intended recipient's independently verifiable data record.

15. (Original) A method according to Claim 13, wherein the releasing step further comprises only releasing the document if the validity of the independently verifiable data record has been confirmed as a result of the check.

16. (Original) A method according to Claim 14, wherein the releasing step further comprises only releasing the document if the validity of the independently verifiable data record has been confirmed as a result of the check.

17. (Previously Presented) A method according to Claim 1, wherein the first and second tokens comprise public and private encryption/decryption keys, respectively, of the intended recipient.

18-20. (Canceled)

21. (Currently Amended) A method of delivering a digital document to an intended recipient at a printout station, the method comprising:

obtaining a first token of ~~the~~ each intended recipient;

encoding the digital document with a session key using a ~~lightweight~~ symmetric cryptographic encryption algorithm, and encrypting the session key with the first token using ~~a computationally heavy~~ an encryption algorithm that is more computationally intensive than the symmetric crytographic encryption algorithm;

receiving and securely retaining the digital document, the encrypted session key and an independently verifiable data record of ~~the~~ each intended recipient at a printout station;

requesting proof of ~~the~~ each intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient;

receiving proof of ~~the~~ each intended recipient's identity in the form of a second token uniquely related to the first token; and

decrypting the encrypted session key with the second token, decoding the digital document with the decrypted session key, and releasing the document, wherein:

the receiving step comprises receiving a plurality of transmitted independently verifiable data records of the intended recipients at the printout station;

the obtaining step comprises obtaining the first tokens of each of the intended recipients;

the requesting step comprises requesting proof of each of the intended recipients' identities at the printout station using data in the independently verifiable data records of the intended recipients; and

the processing step comprises processing each of the intended recipients' response to the request and releasing the document when all of the intended recipients have proved their identity by use of respective second tokens that are each uniquely related to respective ones of the first tokens.

22. (Original) A method according to Claim 21, wherein the transmitted document is a fax document and the printout station comprises a fax machine.

23. (Currently Amended) A method according to Claim 21, wherein the retaining step comprises printing out the document ~~as received~~ and placing it in a locked compartment.

24. (Original) A method according to Claim 23, wherein the releasing step comprises unlocking the compartment where the printed copy of the document is stored.

25. (Original) A method according to Claim 21, wherein the retaining step comprises storing the received document in memory without printing out a copy of it on receipt.

26. (Original) A method according to Claim 25, wherein the releasing step comprises printing out a copy of it.

27. (Original) A method according to Claim 21, wherein the requesting step comprises requesting supply of data encoded with the second token which can be decoded with the first token.

28. (Currently Amended) A method according to Claim 21 wherein the releasing step is carried out when ~~the~~ each intended recipient has presented a portable data carrier holding the second token to the printout station and has transferred data to prove their identity.

29. (Currently Amended) A method according to Claim 28, wherein the releasing step further comprises ~~the~~ each intended recipient entering a verifiable security identifier into the printout station to establish that they are the legitimate owner of the portable data carrier.

30. (Original) A method according to Claim 28, wherein the portable data carrier is a smart card and the printout station comprises a smart card reader.

31. (Original) A method according to Claim 21, wherein the obtaining step comprises extracting the first token transmitted with the document and the data record.

32. (Currently Amended) A method according to Claim 31, wherein ~~the~~ each intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate.

33. (Currently Amended) A method according to Claim 21, further comprising carrying out an on-line check of the validity of ~~the~~ each intended recipient's independently verifiable data record.

34. (Currently Amended) A method according to Claim 21, further comprising instructing a third party to carry out an on-line check of the validity of ~~the~~ each intended recipient's independently verifiable data record.

35. (Currently Amended) A method of according to Claim 33, wherein the releasing step further comprises only releasing the document if the validity of ~~the~~ each independently verifiable data record has been confirmed as a result of the check.

36. (Currently Amended) A method according to Claim 34, wherein the releasing step further comprises only releasing the document if the validity of ~~the~~ each independently verifiable data record has been confirmed as a result of the check.

37. (Currently Amended) A method according to Claim 21, wherein the first and second tokens comprise private and public encryption/decryption keys of the intended recipient.

38. (Canceled)

39. (Currently Amended) A method according to Claim ~~38~~ 21, wherein the transmitted document or a session encryption/decryption key of the transmitted document has been sequentially encrypted with each of the first tokens of the intended recipients in a given order and the processing step comprises sequentially decrypting the transmitted document or a session encryption/decryption key with each of the second tokens of the intended recipients in the reverse of the given sequential order.

40. (Previously Presented) A method of delivering a digital document to intended recipients at a printout station, the method comprising:

receiving and securely retaining a transmitted document at the printout station;

receiving a plurality of independently verifiable data records of the intended recipients at the printout station;

obtaining first tokens of each of the intended recipients;

requesting proof of each of the intended recipient's identities at the printout station using data in the independently verifiable data records of the intended recipients; and

processing each of the intended recipients' responses to the request for proof and releasing the document when all of the intended recipients have proved their identity by use of respective record tokens that are each uniquely related to respective-ones of the first tokens.

41. (Currently Amended) A device for delivering a digital document to an intended recipient, the device comprising:

a communications module for receiving an electronic version of the transmitted document over a communications network, receiving an independently verifiable data record of the intended recipient, and receiving a first token of the intended recipient;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record;

a controller for releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token; ~~and~~

a portable data carrier reader for receiving information from a portable data carrier storing the intended recipient's second token; and

one or more lockable compartments and the device is arranged to print out the document as received and place it in one of the compartments, wherein the controller is arranged to release the locked compartment containing the document, once the intended recipient has proved their identity.

42. (Original) A device according to Claim 41, wherein the device comprises a fax machine.

43. (Previously Presented) A device according to Claim 41, wherein the first and second tokens comprise public and private encryption/decryption keys of the intended recipient.

44-47. (Canceled)

48. (Original) A device according to Claim 41, wherein the controller is arranged to release the received document when the intended recipient has entered a verifiable security identifier into the printout station to establish that they are the legitimate owner of the portable data carrier.

49. (Currently Amended) A device for delivering a digital document to an intended recipient, the device comprising:

a communications module for receiving an electronic version of the transmitted document over a communications network, receiving an independently verifiable data record of the intended recipient, and receiving a first token of the intended recipient;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record;

a controller for releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token; and

one or more lockable compartments and the device is arranged to print out the document as received and place it in one of the compartments.

50. (Original) A device according to Claim 49, wherein the controller is arranged to release the locked compartment containing the document, once the intended recipient has proved their identity.

51. (Original) A device according to Claim 49, wherein the device comprises a fax machine.

52. (Previously Presented) A device according to Claim 49, wherein the first and second tokens comprise public and private encryption/decryption keys of the intended recipient.

53. (Original) A device according to Claim 49, wherein the controller is arranged to release the received document when the intended recipient has entered a verifiable security identifier into the printout station to establish that they are the legitimate owner of a portable data carrier.

54. (Previously Presented) A method of delivering a digital document from a first station via a communications network to an intended recipient at a second station, the method comprising:

obtaining details of the intended recipient, including an independently verifiable data record of the intended recipient at the first station;

determining prior to transmission of the document whether the second station is one which is arranged to implement the present method;

transmitting the document to the second station;

transmitting the independently verifiable data record of the intended recipient to the second station;

receiving and securely retaining the transmitted document and receiving the data record at the second station;

obtaining a first part of an intended recipient's identifying token at the second station;

requesting proof of the intended recipient's identity at the second station using the transmitted independently verifiable data record; and

releasing the document to the intended recipient when the intended recipient has proved their identity using a second part of the recipient's identifying token.

55. (Original) A method according to Claim 54, further comprising obtaining details of the intended recipient including the independently verifiable data record prior to transmitting the document.

56. (Original) A method according to Claim 55, wherein the step of obtaining details comprises obtaining the independently verifiable data record from a central database storing many possible intended recipients' details.

57. (Currently Amended) A method according to ~~any of~~ Claims 54, wherein the intended recipient's independently verifiable data record is provided in an intended recipient's digital certificate.

58. (Currently Amended) A method according to ~~any of Claims~~ Claim 54, further comprising encoding the document prior to transmitting it to the second station and decoding the received document once the intended recipient has proved their identity.

59. (Original) A method according to Claim 58, wherein the encoding/decoding steps comprise using enveloping encryption/decryption techniques.

60-62. (Canceled)

63. (Original) A method according to Claim 60, wherein the intended recipient's independently verifiable data record is provided in an intended recipient's digital certificate.

64. (Previously Presented) A method of delivering a digital document to an intended recipient at a printout station, the method comprising:

obtaining a public token of the intended recipient;

encrypting the digital document with a session key;

encrypting the session key with the intended recipient's public key;

communicating to the printout station and securely retaining the encrypted digital document at the printout station;

communicating the encrypted session key to the printout station;

communicating an independently verifiable data record of the intended recipient to the printout station, the independently verifiable data record comprising the intended recipient's public key;

communicating the independently verifiable data record comprising the intended recipient's public key to a remote device;

decrypting, using a remote device, the encrypted session key using the received intended recipient's public key and an intended recipient's private key residing in the remote device;

communicating the decrypted session key from the remote device to the printout station;

decrypting, at the printout station, the digital document using the decrypted session key; and

releasing the document.

65. (Previously Presented) A method according to Claim 64, wherein the remote device is a smart card configured to communicate with the printout station.